CLAIMS

What is claimed is:

1   1.   A method for detecting modifications to risk assessment scanning caused by
2   an intermediate device, comprising:
3   (a) initiating a risk assessment scan on a target from a remote source utilizing a
4   network;
5   (b) determining whether the risk assessment scan involves an intermediate
6   device coupled between the target and the remote source;
7   (c) receiving results of the risk assessment scan from the target utilizing the
8   network; and
9   (d) notifying an administrator if it is determined that the risk assessment scan
10   involves the intermediate device.

1   2.   The method as recited in claim 1, wherein the intermediate device includes a
2   router.

1   3.   The method as recited in claim 1, wherein the intermediate device includes a
2   proxy server.

1   3.   The method as recited in claim 1, wherein a plurality of procedures are
2   utilized to determine whether the risk assessment scan involves the
3   intermediate device.

1   4.   The method as recited in claim 3, wherein at least one of the procedures
2   includes determining a port list associated with the risk assessment scan.

1   5.   The method as recited in claim 4, wherein the at least one of the procedures

2   further includes determining whether a value of a flag is different for

3   communication attempts using at least two ports on the port list.

1   6.   The method as recited in claim 5, wherein the flag includes an ip_ttl flag.

1   7.   The method as recited in claim 5, wherein the flag includes a tcp_win flag.

1   8.   The method as recited in claim 5, wherein the communications include

2   connection attempts between the remote source and the target utilizing the

3   network.

1   9.   The method as recited in claim 5, wherein the at least one of the procedures

2   further includes indicating that the risk assessment scan involves the

3   intermediate device if the value of the flag is different for the communication

4   attempts using the at least two ports on the port list.

1   10.   The method as recited in claim 3, wherein at least one of the procedures

2   includes transmitting a first request for content to the target utilizing the

3   network, and transmitting a second request for a cached version of the

4   content to the target utilizing the network.

1   11.   The method as recited in claim 10, wherein the cached content is requested

2   from the target utilizing a via tag.

1   12.   The method as recited in claim 10, wherein the at least one of the procedures

2   further includes analyzing responses to the first and second requests.

1   13.   The method as recited in claim 12, wherein the at least one of the procedures

2   further includes indicating that the risk assessment scan involves the

3   intermediate device based on the analysis.

1   14.   The method as recited in claim 13, wherein the at least one of the procedures

2   further includes indicating that the risk assessment scan involves the

3   intermediate device if the responses to the requests are different.

1   15.   The method as recited in claim 3, wherein at least one of the procedures

2   includes transmitting a request without specifying a host header value.

1   16.   The method as recited in claim 15, wherein the at least one of the procedures

2   further includes identifying an error message in response to the request.

1   17.   The method as recited in claim 16, wherein the at least one of the procedures

2   includes indicating that the risk assessment scan involves the intermediate

3   device if the response includes the error message.

1   18.   A computer program product for detecting modifications to risk assessment

2   scanning caused by an intermediate device, comprising:

3   (a)   computer code for initiating a risk assessment scan on a target from a remote

4   source utilizing a network;

5   (b)   computer code for determining whether the risk assessment scan involves an

6   intermediate device coupled between the target and the remote source;

7   (c)   computer code for receiving results of the risk assessment scan from the

8   target utilizing the network; and

9   (d)   computer code for notifying an administrator if it is determined that the risk

10   assessment scan involves the intermediate device.

1   19.   The computer program product as recited in claim 18, wherein the

2   intermediate device includes a router.

1   20.   The computer program product as recited in claim 18, wherein the

2   intermediate device includes a proxy server.

1   21.   The computer program product as recited in claim 18, wherein a plurality of
2   procedures are utilized to determine whether the risk assessment scan
3   involves the intermediate device.

1   22.   The computer program product as recited in claim 21, wherein at least one of
2   the procedures includes determining a port list associated with the risk
3   assessment scan.

1   23.   The computer program product as recited in claim 22, wherein the at least
2   one of the procedures further includes determining whether a value of a flag
3   is different for communication attempts using at least two ports on the port
4   list.

1   24.   The computer program product as recited in claim 23, wherein the flag
2   includes an ip_ttl flag.

1   25.   The computer program product as recited in claim 23, wherein the flag
2   includes a tcp_win flag.

1   26.   The computer program product as recited in claim 23, wherein the
2   communications include connection attempts between the remote source and
3   the target utilizing the network.

1   27.   The computer program product as recited in claim 23, wherein the at least
2   one of the procedures further includes indicating that the risk assessment
3   scan involves the intermediate device if the value of the flag is different for
4   the communication attempts using the at least two ports on the port list.

1   28.   The computer program product as recited in claim 21, wherein at least one of
2   the procedures includes transmitting a first request for content to the target

3   utilizing the network, and transmitting a second request for a cached version

4   of the content to the target utilizing the network.

1   29.   The computer program product as recited in claim 28, wherein the cached

2   content is requested from the target utilizing a via tag.

1   30.   The computer program product as recited in claim 28, wherein the at least

2   one of the procedures further includes analyzing responses to the first and

3   second requests.

1   31.   The computer program product as recited in claim 30, wherein the at least

2   one of the procedures further includes indicating that the risk assessment

3   scan involves the intermediate device based on the analysis.

1   32.   The computer program product as recited in claim 31, wherein the at least

2   one of the procedures further includes indicating that the risk assessment

3   scan involves the intermediate device if the responses to the requests are

4   different.

1   33.   The computer program product as recited in claim 21, wherein at least one of

2   the procedures includes transmitting a request without specifying a host

3   header value.

1   34.   The computer program product as recited in claim 33, wherein the at least

2   one of the procedures further includes identifying an error message in

3   response to the request.

1   35.   The computer program product as recited in claim 34, wherein the at least

2   one of the procedures includes indicating that the risk assessment scan

3   involves the intermediate device if the response includes the error message.

1   36.   A system for detecting modifications to risk assessment scanning caused by

2   an intermediate device, comprising:

3   (a)   logic for initiating a risk assessment scan on a target from a remote source

4   utilizing a network;

5   (b)   logic for determining whether the risk assessment scan involves an

6   intermediate device coupled between the target and the remote source;

7   (c)   logic for receiving results of the risk assessment scan from the target utilizing

8   the network; and

9   (d)   logic for notifying an administrator if it is determined that the risk

10   assessment scan involves the intermediate device.

1   37.   A method for detecting modifications to risk assessment scanning caused by

2   a proxy server, comprising:

3   (a)   initiating a risk assessment scan on a target from a remote source utilizing a

4   network;

5   (b)   executing a plurality of procedures to determining whether the risk

6   assessment scan involves a proxy server coupled between the target and the

7   remote source;

8   (c)   said procedures utilizing a plurality of parameters selected from the group

9   consisting of an ip_ttl flag, a tcp_win flag, a via tag, and a host header value;

10   (d)   receiving results of the risk assessment scan from the target utilizing the

11   network;

12   (e)   flagging the results of the risk assessment scan if at least one of the

13   procedures indicates that the risk assessment scan involves a proxy server

14   coupled between the target and the remote source; and

15   (f)   notifying an administrator if the results of the risk assessment scan are

16   flagged.

1   38.   A computer program product for detecting modifications to risk assessment

2   scanning caused by a proxy server, comprising:

3	(a)	computer code for initiating a risk assessment scan on a target from a remote
4		source utilizing a network;
5	(b)	computer code for executing a plurality of procedures to determining
6		whether the risk assessment scan involves a proxy server coupled between
7		the target and the remote source;
8	(c)	said procedures utilizing a plurality of parameters selected from the group
9		consisting of an ip_ttl flag, a tcp_win flag, a via tag, and a host header value;
10	(d)	computer code for receiving results of the risk assessment scan from the
11		target utilizing the network;
12	(e)	computer code for flagging the results of the risk assessment scan if at least
13		one of the procedures indicates that the risk assessment scan involves a proxy
14		server coupled between the target and the remote source;
15	(f)	computer code for notifying an administrator if the results of the risk
16		assessment scan are flagged.